# STEGANOGRAPHIC PROGRAM WITH A GRAPHICAL INTERFACE FOR DATA PROTECTION IN SOCIAL NETWORKS

**HRISTO I. PARASKEVOV, EKREM D. MEHMEDOV**

***ABSTRACT:*** *The article offers different combinations of cryptographic and steganographic algorithms. The cryptographic algorithms of Caesar, Fernet and RSA are considered and programmatically implemented. The LSB method was used as a basis for the steganographic algorithms, as it was used in various modifications in order to increase the invisibility and detectability of the hidden message. Experimental results show that the use of a combination of cryptographic and steganographic algorithms on social networks increases the security and undetectability of secret messages.*

***KEYWORDS:*** *Steganography, social networks, information security*

***DOI:*** https://doi.org/10.46687/JNVU5241

# СТЕГАНОГРАФСКА ПРОГРАМА С ГРАФИЧЕН ИНТЕРФЕЙС ЗА ЗАЩИТА НА ДАННИ В СОЦИАЛНИ МРЕЖИ*

**ХРИСТО ИВ. ПАРАСКЕВОВ, ЕКРЕМ ДЖ. МЕХМЕДОВ**

***АБСТРАКТ*** *В статията се предлагат различни комбинации от криптографски и стеганографски алгоритми. Разгледани и програмно реализирани са криптографските алгоритми на Цезар, Фернет и RSA. За основа на стеганографските алгоритми е използван LSB методът, като е използван в различни модификации с цел увеличаване на незабележимостта и откриваемостта на скритото съобщение. Експерименталните резултати показват, че прилагането в социални мрежи на комбинация между криптографските и стеганографските алгоритми повишават защитеността и неоткриваемостта на секретните съобщения.*.

## 1 Въведение

Конфиденциалността и сигурността на информацията са основна необходимост в човешката история и ежедневие. Хората колкото и да решават тази необходимост със средствата на криптографията, те не изключват вероятността информацията и/или нейното предаване, да бъде забелязано и да се атакува чрез груба сила и/или други атаки. В такива ситуации е възможно да се използват методите на стеганографията, науката за скриване на информацията.

В 21-ви век, светът, който ни заобикаля е забързан и модернистичен, предлага много възможности, и то на клик разстояние. Едно нещо е сигурно, че винаги ще се използва и ще има нужда от комуникация. Всяко човешко същество има право на комуникация, без каквито и да е било ограничения и място на осъществяването й. Остава въпроса дали тази комуникация е сигурна и надеждна. Тъй като съвременният живот с всеки изминал ден става все по-динамичен, това налага непрекъснат пренос или обмен на данни между потребителите, включително и през социални медии. И колкото и да се набляга на сигурността на комуникационният канал между потребителите, използващи дадена

* Настоящата статия е частично финансирана по проект № РД-08-147/02.03.2022.

социална медия, то винаги има риск, то този комуникационен канал да попада в ръцете на неподходящи лица.

Социалните медии са трудно дефинитивно определими, защото са образувани от различни потребители и организации, взаимодействащи помежду си на интернет платформи. Една от основните им характеристика е тяхното непостоянство и видоизменянето на приложението им. Но най-общо казано социалните медии могат да се определят като сайтове, които се попълват със съдържание от самите потребители. За разлика от традиционните медии, в които журналисти и редактори на щат решават каква информация да бъде публикувана и каква информация – не, в социалните медии хората решават това и просто го правят. Те са мястото, което предоставят възможността на потребителите да създават взаимоотношения и бърза връзка с цел комуникация.

Криптографията е наука, включваща набор от математически действия, с помощта на които се създават дефиниции като поверителност, удостоверяване и защита на данни, които са предназначени да защитават и осигуряват наличността на данни при кореспонденция на изпращач и получател. Тя защитава данните от атаки, като преобразува информацията, съдържаща се в обикновеният текст, така че тя да е невъзможна за четене без ключова информация [1]. Криптографските алгоритмите се делят основно на три група: заместване(substitution), разместване(transposition), и алгебрични. Тези техники могат да се използват отделно или в комбинация в процесите на криптиране [2].

Стеганографските методи и алгоритми осигуряват поверително предаване на данни, без да се забелязва от трети лица. Днес стеганографията е наука, която има за цел да скрие факта на съществуването на тайни съобщения или информация, които се предават без подозрението от трети лица. Такива данни може да се скриват в текст, в графични файлови формати, в аудио и видео файлови формати [3, 4]. От формулирането на класическия затворнически проблем [5] измина време, в което стеганографските методи се съчетаха с криптографски, биологични и много други области, за да може да се получи все по-добрата стеганографска система. Съществуват различни комбинации, в които стеганографията и криптографията се сътрудничат за осъществяване на по-добра устойчивост на данните, за намаляване на вмъкваната информация и разбира се за увеличаване на незебележимостта на скритата информация. Подобни примери са описани в [6, 7 и 8], като и във всички случаи се касае за стеганографски методи, при които стегофайлът не променя своите размери, спрямо контейнера.

# 2 Описание на алгоритмите, използвани в предложената програма

2.1. Криптографски алгоритми

Алгоритъм на Цезар

Алгоритъмът на Цезар представлява програмно решение на метода Цезар криптиране, съответно и декриптиране чрез математически, булеви и други програмни изрази, които позволяват постигане на резултат по поставените задачи за решение.

Алгоритъм на Фернет

Този алгоритъм е от семейството на симетрично криптиращите алгоритми, при които се използва един и същ генериран ключ за криптиране и декриптиране. Алгоритъмът на Фернет гарантира, че данните, криптирани с него, не могат да бъдат допълнително манипулирани или четени без ключа. След посочването на откритият текст, алгоритъмът на Фернет генерира ключ, който още се нарича жетон на Фернет. След това се осъществява криптирането на текста с помощта на ключа. Декриптирането се осъществява по обратния ред със същият ключ.

Алгоритъм RSA

Този алгоритъм е един от най-известните криптиращи алгоритми, най-вероятно няма голяма търговска компания, която да не го използва при своите комуникации, а най-вече при защита на данни. Алгоритъмът се основава на криптиране чрез използване факторизация на простите числа. Самият алгоритъм започва с подаване на прав текст и две произволни прости числа, тези числа се модифицират чрез математически изчисления, докато не се получи публичния и частния ключ. Публичният ключ служи за да се криптира правият текст. А частният ключ за декриптиране на криптираният текст.

2.2. Стеганографски алгоритми

Модифициран LSB алгоритъм (Red, Green и Blue)

Основен алгоритъм за вграждане/извличане на поверителна информация в/от цифрови изображение чрез използване на трите канала на пикселите, а и с възможност за прескачания на пиксели.

Модифициран LSB алгоритъм (Red и Green)

Модифициран алгоритъм на основния алгоритъм за вграждане/извличане на поверителна информация в/от цифрови изображение чрез използване на двата канала на пикселите, а и с възможност за прескачания на пиксели.

Модифициран LSB алгоритъм (Red и Blue)

Модифициран алгоритъм на основния алгоритъм за вграждане/извличане на поверителна информация в/от цифрови изображение чрез използване на двата канала на пикселите, а и с възможност за прескачания на пиксели.

Модифициран LSB алгоритъм (Green и Blue)

Модифициран алгоритъм на основния алгоритъм за вграждане/извличане на поверителна информация в/от цифрови изображение чрез използване на двата канала на пикселите, а и с възможност за прескачания на пиксели.

## 3 Избор на показатели за оценка на резултатите

При оценяване на резултатите се отчитат няколко показателя:

1) Първото изследване е визуална оценка между оригиналните изображения и стегофайловете. Ако се отчете значителна промяна във визуалното качество на стегофайла, е необходимо да се извърши задължителна промяна в стеганографския алгоритъм.

2) Освен визуалните промени е необходимо да се сравняват и статистическите свойства на получените стегофайлове. По този начин могат да се отчетат леки промени на цветовете, които човешкото око не е способно да забележи.

3) PSNR изчислява пиковото съотношение сигнал-шум, в децибели, между двете изображения. Това съотношение се използва често като измерване на качеството между оригинално и променено изображение. Колкото по-високи са стойностите на PSNR, толкова е промените са по- незабележими.

За да се изчисли PSNR, първо се изчислява средната квадратична грешка MSE с помощта на следния израз:

(1) $$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)\|^2$$

където:

m,n – размерността на изображението
f(i,j) – пиксел от оригиналното изображение
gf(i,j) – пиксел от промененото изображение

(2) $$PSNR = 20\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right)$$

където:
$MAX_f$ – максималната стойност, която се използва за идентифициране на цвят.

# 4 Експериментални резултати

**Експеримент 1:**

**Стеганографски алгоритми чрез Цезар криптиране на съобщение**

1) Избраният контейнер е от личен архив с размери 1080x810 (фиг.1), в който се вгражда съобщение с дължина 1423 байта, в битове тази стойност се явява 11 384, самото вграждане се осъществява през 20 пиксела. MSE и PSNR стойностите при сравняване на контейнера със стего файла (фиг.2) съответно са 0,0074 и 72,70 .

**Фиг.1. Контейнер**

**Фиг.2 Стего файл**

2) Чрез стеганографският алгоритъм LSB(RG) на програмната реализация „StegoCrypt“. В контейнер от личен архив с размери 1080x810 (фиг.3) се вгражда съобщение с дължина 1423 байта, в битове тази стойност се явява 11 384, самото вграждане се осъществява през 20 пиксела. MSE и PSNR стойностите при сравняване на контейнера със стего файла (фиг.4) съответно са 0,0072 и 71,29.

**Фиг.3. Контейнер**

**Фиг.4 Стего файл**

**Таблица 1 Стойности на MSE и PSNR**

| СТЕГАНОГРАФСКИ АЛГОРИТЪМ | КОНТЕЙНЕР | СТЕГОФАЙЛ | MSE | PSNR |
|---|---|---|---|---|
| LSB(RGB) | #1 | #1 | 0,0074 | 72,70 |
| LSB(RG) | #2 | #2 | 0,0072 | 71,29 |

**Експеримент 2:**

**Стеганографски алгоритми чрез Фернет криптиране на съобщение**

1) Чрез стеганографският алгоритъм LSB(RGB) на програмната реализация „StegoCrypt“. В контейнер от личен архив с размери 1080x810 (фиг.5) се вгражда съобщение с дължина 485 байта, в битове тази стойност се явява 3 880, самото вграждане се осъществява през 20 пиксела. MSE и PSNR на контейнера със стего файла (фиг.6) съответно са 0,0080 и 71,35 .

**Фиг.5. Контейнер**

**Фиг.6 Стего файл**

**Таблица 2 Стойности на MSE и PSNR**

| СТЕГАНОГРАФСКИ АЛГОРИТЪМ | КОНТЕЙНЕР | СТЕГОФАЙЛ | MSE | PSNR |
|---|---|---|---|---|
| LSB(RGB) | #3 | #3 | 0,0080 | 71,35 |
| LSB(RG) | #4 | #4 | 0,0330 | 66,04 |

2) Чрез стеганографският алгоритъм LSB(RGB) на програмната реализация „StegoCrypt“. В контейнер от личен архив с размери 1080x810 (фиг.7) се вгражда съобщение с дължина 485 байта, в битове тази стойност се явява 3 880, самото вграждане се осъществява през 20 пиксела. MSE(mean squared error), тоест средната квадратичната грешка и PSNR на контейнера със стего файла(фиг.8) съответно са 0,0330 и 66,04.

**Фиг.7. Контейнер**

**Фиг.8 Стего файл**

**Експеримент 3:**

**Стеганографски алгоритми чрез RSA криптиране на съобщение**

1) Чрез стеганографският алгоритъм LSB(RGB) на програмната реализация „StegoCrypt“. На контейнер от личен архив с размери 1080x810 (фиг.9) се вгражда съобщение с дължина 5405 байта, в битове тази стойност се явява 43 240, самото вграждане се осъществява през 15 пиксела. MSE и PSNR на контейнера със стего файла (фиг.10) съответно са 0,0330 и 66,02 .

**Фиг.9. Контейнер**

**Фиг.10 Стего файл**

1) Чрез стеганографският алгоритъм LSB(RGB) на програмната реализация „StegoCrypt“. В контейнер от личен архив с размери 1080x810 (фиг.11) се вгражда съобщение с дължина 5405 байта, в битове тази стойност се явява 43 240, самото вграждане се осъществява през 10 пиксела. MSE и PSNR на контейнера със стего файла (фиг.12) съответно са 0,0462 и 64,02.

**Таблица 3 Стойности на MSE и PSNR**

| СТЕГАНОГРАФСКИ АЛГОРИТЪМ | КОНТЕЙНЕР | СТЕГОФАЙЛ | MSE | PSNR |
|---|---|---|---|---|
| LSB(RGB) | #5 | #5 | 0,0330 | 66,02 |
| LSB(RG) | #6 | #6 | 0,0462 | 64,02 |

**Фиг.11. Контейнер**

**Фиг.12 Стего файл**

# 5 Заключение

Изследванията на програмната реализация, показват стабилността на избраните стеганографски алгоритми с допълнителната сигурност на поверителната информация, чрез избраните криптографските алгоритми. Експерименталните резултати показват сходни крайни стойности на оценяваните параметри, като при стеганографските методи с криптиране с модифицирания метод на Цезар се получават най-добри резултати. Получената реализация е подходяща за научни изследвания в сферата на стеганографията и криптографията, тъй като предлага отделни функционалности за тях, но най-вече тази разработка е подходяща за обучение на студенти.

**ЛИТЕРАТУРА:**


[1] Yılmaz, R. ,“Kriptolojik Uygulamalarda Bazı İstatistik Testler”, YüksekLisans Tezi, Selçuk Üniversitesi Fen Bilimleri Enstitüsü, Konya, 1-31(2010).

[2] Başar, M.S., “Yer Değiştirme Esaslı ve Rasgele Anahtarlı Yeni Bir Şifreleme,Algoritması”, Doktora Tezi, Atatürk Üniversitesi SosyalBilimler Enstitüsü,Erzurum, 1-17 (2004).

[3] Memon N., Wong, P.1998.“Protecting digital media content”, Communications of the ACM, vol 41, no. 7 , pp. 34–43.

[4] Wang H., Wang S.1984.“Cyber Warfare: Steganography vs. Steganalysis”, Communications of the ACM, vol. 47, no. 10, October 2004.

[5] Simmons G.1984, “The Prisoners' Problem and the Subliminal Channel", CRYPTO83 Advances in Cryptology, pp. 51-67.

[6] R. Dumre and A. Dave, "Exploring LSB Steganography Possibilities in RGB Images," *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2021, pp. 1-7, doi: 10.1109/ICCCNT51525.2021.9579588.

[7] Kiliroor, C.C., Neelam, T., Bhagat, K. (2022). Coalescing Image Steganography and Cryptography for Information Security. In: Saraswat, M., Roy, S., Chowdhury, C., Gandomi, A.H. (eds) Proceedings of International Conference on Data Science and Applications . Lecture Notes in Networks and Systems, vol 288. Springer, Singapore. https://doi.org/10.1007/978-981-16-5120-5_28

[8] Paraskevov, Hristo, Georgi Valchev, and Radostin Rafailov. "Steganographic algorithm in video with message encryption." *AIP Conference Proceedings*. Vol. 2505. No. 1. AIP Publishing LLC, 2022.